

AWIPS SYSTEM ADMINISTRATION NOTE 16 (for Electronics Technicians)
Maintenance, Logistics, and Acquisition Division
W/OPS12: JCS

SUBJECT : Passing SSH traffic through gauntlet firewall

PURPOSE : To reconfigure the AWIPS/LDAD firewall to pass SSH traffic

EQUIPMENT : AWIPS Gauntlet Firewall
AFFECTED

EFFECTIVITY : All AWIPS sites with a gauntlet firewall.

ESTIMATED TIME : 30-45 minutes
REQUIRED

EFFECT ON OTHER : None. File in EHB-13, section 2.0

INSTRUCTIONS

VERIFICATION : This procedure has been tested and verified at National Regional
STATEMENT Headquarters, Silver Spring, MD (SLVM2)

GENERAL:

The following procedure will:

- Ensure that there is an entry for ssh in gw:/etc/services.
- Ensure that there is an entry for ssh in gw:/etc/inetd.conf.
- Back up gw:/usr/local/etc/netperm-table to /usr/local/etc/netperm-table.preSSH.
- Add ssh entries to gw:/usr/local/etc/netperm-table.
- Back up gw:/etc/scripts/updt_table to gw:/etc/scripts/updt_table.preSSH.
- Add ssh entries to gw:/etc/scripts/updt_table.

Performing a backup of the LDAD is recommended at this time. The instructions for performing an LDAD backup are located at:

http://www.ops1.nws.noaa.gov/awipsnew/software/sysadmin12_ldad_bkup_S.pdf

PROCEDURE:

NOTE: OB2 **must be installed** prior to performing these procedures.

Logging into the firewall:

The procedures below are utilized by the SST/NCF technical support to log into the gauntlet firewall server from the DS1 server. Logging in from the system console to the gauntlet firewall server can be used as an alternate method of login.

1. After logging into DS1, type the following in the telnet window:

```
export TERM=vt100
telnet xyplex1 2000
```

The message displays:

```
Trying...
Connected to xyplex1.
Escape character is '^['.
```

2. Press **Enter** to get a # prompt from the AWIPS xyplex. At the # prompt, type:
access (the word `access` will not be displayed as you type it in)

Press **Enter**

3. After the access password is entered, the AWIPS xyplex displays the following:

```
Welcome to AWIPS
Enter username>
```

At the `Enter username>` prompt, type **awips** and press **Enter**.

4. At the `Xyplex>` prompt, type:

```
c xyplex1:5800
```

Press **Enter** twice to obtain a login prompt from the gauntlet firewall server.

5. The following message displays:

```
Xyplex -010- Session 1 to XYPLEX1:5800 established
The Gauntlet(R) Internet Firewall V4.1 -- By Trusted Information
Systems
gw-nhda.nws.noaa.gov
login:
```

Login as `root` and type the password to enter the gauntlet firewall server.

Reconfiguring the firewall:6. Change directory to `/etc/scripts` by typing:

```
cd /etc/scripts
```

7. Make an FTP connection to NOAA1 and get the `configSSH.sh` script by typing the commands in **bold**:

```
ftp 165.92.25.15
Name (165.92.25.15:root): ftp
331 Guest login ok, send your complete e-mail address as password.
password: your.name@noaa.gov
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /pub
250 CWD command successful.
ftp> get configSSH.sh
200 PORT command successful.
150 Opened BINARY mode data connection for configSSH.sh (4343
bytes)
226 Transfer complete
4343 bytes received in 0.01 seconds (670.34 Kbytes/s)
ftp> quit
221 Goodbye
```

8. Make the script executable and run it by typing:

```
chmod 555 configSSH.sh
./configSSH.sh
```

9. To restart the networking software, type:

```
reboot
```

10. To verify that SSH has been successfully configured on the firewall, initiate an SSH session from DS1 to LS1. As the `root` user on the DS1 server, type the following:

```
ds1-nhda {root}# ssh ls1
```

If SSH has been successfully configured on the firewall, you should receive a password prompt from LS1. Next, type the `root` user's password for LS1 and verify that you have successfully logged into LS1.

This completes the gauntlet firewall reconfiguration procedure.

NOTE: A webpage of FAQs regarding questions about the AWIPS implementation of secure shell has been set up at the following URL:
http://www.ops1.nws.noaa.gov/awips_install.htm

REPORTING INSTRUCTIONS:

Report the completed modification using the Engineering Management Reporting System (EMRS) according to the instructions in NWS Instruction 30-2104, Maintenance Documentation, Part 4, Appendix F. Include the following information on the EMRS Report:

Block #	Block Type	Information
5	Description	Reconfigure the AWIPS/LDAD firewall to pass SSH traffic
7	Equipment Code	AWIPS
8	Serial Number	001
15	Comments	Reconfigured the AWIPS/LDAD firewall I.A.W. AWIPS Sys Admin Note 16
17a	Mod. No.	SA16

Mark S. Paese
Director, Maintenance, Logistics, and Acquisition Division

Attachment A - EMRS Report Sample

Attachment A - Sample EMRS Report

A26 Detail Form - ESCM2, SILVER SPRING, MD :: JOHN MERHI - Microsoft Internet Explorer

New A26 Commit A26 Place on Hold Copy A26 Delete A26 Detail Report Document Summary Help

GENERAL INFORMATION

NEW RECORD WFO* TBW Document No.* TBW31112001

1. Open Date: 11/12/2003 Open Time: 09:00 2. Op Initials: WSH 3. Response Priority: ☐ Immediate ☐ Low ☐ Routine ☒ Not Applicable 4. Close Date: 11/12/2003 Close Time: 10:00

5. Maintenance Description: 445 characters left AWIPS
Reconfigure the AWIPS/LDAD firewall to pass SSH traffic

EQUIPMENT INFORMATION

6. Station ID*: TBW 7. Equipment Code: AWIPS 8. Serial Number: 001 9. TM: M 10. AT: M 11. How Mal: 999

Alert: Time Remaining: (For Block 12 use only)

13. PARTS USAGE and CONFIGURATION MANAGEMENT REPORTING

ASN	Vendor Part No. (New Part)	Serial Number (Old Part)	Serial Number (New Part)	
				New Row
				Delete Row

14. WORKLOAD INFORMATION

a. Routine	b. Non-Routine	c. Travel	d. Misc	e. Overtime
Hours Minutes	Hours Minutes	Hours Minutes	Hours Minutes	Hours Minutes
			0 45	

MISCELLANEOUS INFORMATION

15. Maintenance Comments: 683 characters left
Reconfigured the AWIPS/LDAD firewall I.A.W. AWIPS Sys Admin Note 16

16. Tech Initials: GAF

17. SPECIAL PURPOSE REPORTING INFORMATION

a. Mod No.	b. Mod Act/Deact Date	c. Block C	d. Trouble Ticket No.	e. Block E
SA16	11/12/2003			

Commit A26 Place on Hold Copy A26 New A26 Cancel

Done Internet